HP OpenView

Storage Mirroring application notes

High availability for Exchange Server 2000/2003

Part number: T2558–88020
Second edition: May 2005

Legal and notice information

Storage Mirroring High availability for Exchange Server 2000/2003 application notes

Introduction

Microsoft Exchange Server is a messaging and collaboration server for the most demanding business needs. Its scalability, performance, and enhanced security make Exchange an ideal messaging foundation for enterprise networks. Storage Mirroring provides real-time enterprise data protection and replication. Storage Mirroring can be used to provide high availability for your Exchange server.

This document describes the steps necessary to configure Storage Mirroring to provide high availability for Windows servers running Microsoft Exchange Server version 2000 or 2003. These procedures allow a secondary server to assume the identity and role of a failed Exchange server while maintaining the availability of Exchange services with minimal disruption or data loss. That means that users will have access to the same mailboxes and public folders on a uniquely-named target server that existed on the source server prior to a failure.

In addition to the Exchange Information Stores (mailboxes and public folders), there are many important aspects of an Exchange server configuration that are required for Exchange functionality following the loss of a production Exchange Server. It is important to be aware of the overall production Exchange server configuration and to configure the target server identically. Some configuration aspects fall outside the scope of this document such as the configuration of any Exchange Connectors, Built-In Instant Messaging, Newsgroups, Bridgehead Servers, and so on. These issues need to be addressed exclusively by the Exchange administrator.

To complete these instructions, you will install Microsoft Exchange Server and Storage Mirroring, then configure Storage Mirroring for replication and failover. Due to the complexities of these applications, this document is intended for network administrators with experience installing, configuring, and maintaining network applications, including Storage Mirroring and Microsoft Exchange Server. This document is not intended for Exchange running on Microsoft Cluster Service. It is for configurations with Exchange running on member servers.

Requirements

- Two servers that meet one of the following operating system requirements:
  - Microsoft Windows 2000 Service Pack 4 or later
  - Microsoft Windows 2003

NOTE: The source and target servers must both be running the same operating system.

- Two licensed copies of Microsoft Exchange Server that meet one of the following requirements:
  - Exchange Server 2000 with Service Pack 3 or higher
  - Exchange Server 2003

NOTE: HP recommends that the Exchange version be the same as the operating system version.

- Two licensed copies of Storage Mirroring version 4.3.4 or later
- A copy of the Exchange Failover utility (`exchfailover.exe`) version 2.1.

NOTE: If you are upgrading from an earlier version of the Exchange Failover utility, you will need to do the following:

- Compare the sample scripts to your failback and post-restore scripts and incorporate the new commands (`-nopublicfolders`, `-onlypublicfolders`) into your scripts.
- Modify the failover and failback scripts to remove the NSISPN commands. This functionality has been incorporated into the utility and is no longer necessary in the scripts. Leaving the commands in the scripts will not cause any harm or failure in execution.

- Domain structure—The two Exchange servers must have the same root domain.

NOTE: If you are using a WAN environment (the source and target are on different subnets), see "Appendix 1: WAN configuration" on page 21 for additional requirements and specific WAN configuration steps.

Backing up your environment

Before beginning these procedures, make sure you have a current backup of your source and target. Also, make sure you have a complete backup of Active Directory.

Environment verification

Before you use the Exchange Failover utility, complete the following tasks to verify that the environment is properly set up.

1. With both Exchange servers online, use Active Directory Users and Computers to move an existing user from the source to the target and then back to the original source.
2. Verify that you can create a new user on the target.
3. To verify connectivity, create an Outlook profile for the new user on a client machine and connect to the target.

Protecting your exchange data

Protecting your Exchange data requires four separate procedures. You must complete each section before your data will be protected.

- "Preparing the source server" on page 5 includes the installation and preparation instructions for the source.
- "Preparing the target server" on page 6 installs software on the target and configures Exchange on the target.
- "Configuring Storage Mirroring mirroring and replication" on page 8 walks you through creating your Storage Mirroring replication set and establishing the Storage Mirroring connection between your source and target servers.
- "Configuring failure monitoring" on page 9 establishes high availability by configuring Storage Mirroring failure monitoring.

Preparing the source server

In this section, you will be configuring the source and installing software.

1. Configure the source as a Windows 200x member server.

Windows member server

2. Apply any Windows 200x service packs or patches.
3. Install Exchange 200x on the source, if it is not already installed.

Windows member server
Exchange

NOTE: Keep track of your installation selections and storage locations so that Exchange can be installed identically on the target. You will need to know the exact names and locations for the following items:

- Storage group names
- Public store name
- Private store name
- Log files and system paths
- Log file prefix
- Database names
- Database paths

4. Apply any Exchange service packs or patches. Exchange 2000 requires Service Pack 3 or later.
5. Install Storage Mirroring, if it is not already installed.

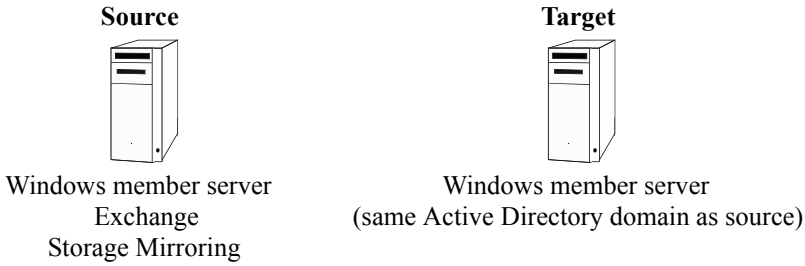
Windows member server
Exchange
Storage Mirroring

6. Run the `setup.exe` file to install the Exchange Failover utility in the Storage Mirroring directory on the source.

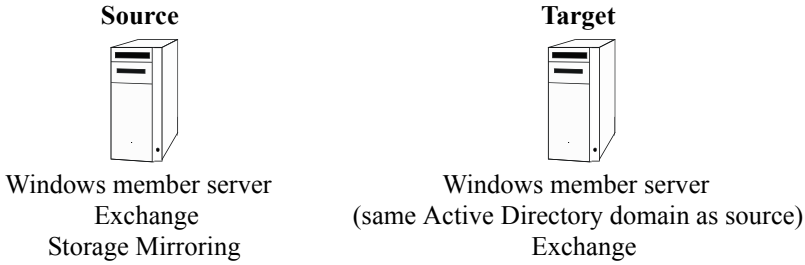
Preparing the target server

In this section, you will be installing software on the target and configuring Exchange on the target.

1. Configure the target as a Windows 200x member server in the same Active Directory domain as the source.



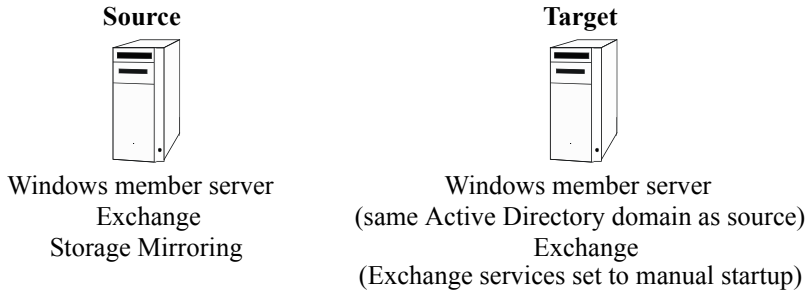
2. Apply any Windows 200x service packs or patches.
3. Install Exchange 200x on the target placing it in the same Exchange organization as the source and verifying that the installation locations are the same as the source.



4. Apply any Exchange service packs or patches. Exchange 2000 requires Service Pack 3 or later.

NOTE: Make sure that your Exchange installation selections and storage locations on the target are the same as the source.

5. On the target, change the Exchange services that are automatic startup to manual startup. If an Exchange service is disabled because it is not necessary for your environment, leave the service disabled. Listed below are Exchange services. Not all services may be used or present in your environment depending on your Exchange version.
   - Microsoft Exchange System Attendant (MSExchangeSA)
   - Microsoft Exchange Information Store (MSExchangeIS)
   - Microsoft Exchange Event Service (MSExchangeES)
   - Microsoft Exchange MTA Stacks (MSExchangeMTA)
   - Microsoft Exchange Post Office Protocol (POP3Svc)
   - Microsoft Exchange Internet Message Access Protocol (IMAP4Svc)
   - Microsoft Exchange Management (MSExchangeMGMT)
   - Microsoft Exchange Routing Engine (RESvc)
   - Any other Exchange related services: Fax, Blackberry, Management software, and so on.



6. When you installed Exchange on the source, the default Exchange storage group was assigned `E00` as the prefix of the log files. The second storage group was assigned `E01`, the third `E02`, and so on. The storage groups on the target must have the same numbering scheme. If you have one or two storage groups on your source, you can continue with the next step. If you have more than two storage groups on your source, verify that the prefix numbering is the same on the source and target.

   a. Using Exchange System Manager on the source, select the source Exchange server. Right-click each storage group and select **Properties**. Record the prefix number assigned to each storage group.

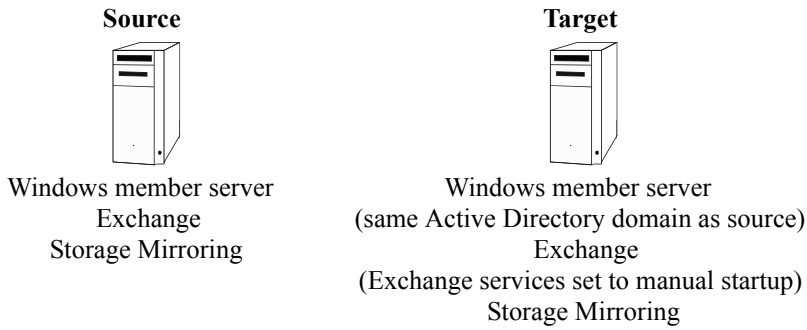
   b. On the target, use Exchange System Manager to verify the prefix number assigned to each storage group.

      If the storage group prefix numbers are identical, you can continue with the next step. If the storage group prefix numbers are different, you will need to modify them. You can do this by deleting the storage groups and re-creating them in the same order they were created on the source, or you can use ADSIEdit to modify the prefix numbers. Using ADSIEdit, modify the properties of the entry noted below to change the `msExchESEParamBaseName` on the Properties page to match that of the source. The entry that must be edited is

      ```
      CN=First_Storage_Group_Name, CN=Information Store,
      CN=Exchange_Server_Name, CN=Servers,
      CN=First_Administrative_Group_Name, CN=Administrative Groups,
      CN=Exchange_Organizational_Name, CN=Microsoft Exchange, CN=Services,
      CN=Configuration, DC=Domain_name, DC=com
      ```

      You will have to use ADSIEdit from the Windows Support Tools to make this change. See your Windows reference guide for more information.

7. Install Storage Mirroring on the target and reboot when the installation is complete. This will initialize Storage Mirroring and stop the Exchange services because the services are set to manual.



8. Run the `setup.exe` file to install the Exchange Failover utility in the Storage Mirroring directory on the target.

Configuring Storage Mirroring mirroring and replication

In this section, you will be creating your Storage Mirroring replication set and establishing the Storage Mirroring connection between your source and target servers.

1. On the source, open the Storage Mirroring Management Console (**Start**, **Programs**, **Storage Mirroring**, **Management Console**).
2. In the left pane of the Management Console, double-click on the target to login.
3. Again in the left pane, double-click on the source to login.
4. Right-click on the source and select **Properties**.
5. On the Source tab, enable **Block Checksum All Files on a Difference Mirror** and click **OK**.
6. Right-click the source and select **New**, **Replication Set** and enter the desired name for the replication set.
7. Select your Exchange data to replicate to the target. You can use the GUI selection process or the Replication Set Properties dialog box. See the *HP OpenView Storage Mirroring user's guide* for information on creating replication set rules.

NOTE: Be sure of the following caveats:

- Select the drive(s) and/or directories that contain the Exchange database and log files. The `MDBDATA`, `MAILROOT`, and `MTADATA` directories must be included.
- Exclude the `\bin` directory.
- Exclude any application files (`.dll` and `.exe`) since Exchange is already installed on the target.

When creating a rule that excludes files based on a wildcard, you must include the full path to the wildcard. For example, to exclude all `.dll` files in the `exchsrvr` directory, the replication set rule should be `c:\program files\exchsrvr\*.dll`. See the *HP OpenView Storage Mirroring user's guide* for information on creating replication set rules.

---

8. Right-click the replication set name and select **Save** to save the replication set.
9. Drag and drop the replication set onto the target and the Connection Manager will open.
10. The **Source Server**, **Target Server**, **Replication Set**, and **Route** fields will automatically be populated. If you have multiple IP addresses on your target, verify the **Route** field is set to the correct network path. (For detailed information on establishing a connection, see the *HP OpenView Storage Mirroring user's guide*.)
11. Select **One to One** to map the replication set data from the source to an identical volume/directory structure on the target.
12. **On the Orphans tab, select to move or delete orphan files on the source.** Orphan files, such as out-dated transaction logs, may keep the database from starting on the source. For more information about orphan files, see the *HP OpenView Storage Mirroring user's guide*.
13. Click **Connect** to start the mirror and replication processes.

Exchange continuously writes data to the disk, which causes the replication statistics in the Storage Mirroring Management Console to constantly change, even when users are not logged in.

Your data is protected after the mirror is complete and the **Mirror Status** has changed to **Idle**.

NOTE: If you start Exchange Server and mount the replicated databases on the target, or if the data on the target is otherwise modified, the data on the source and target will no longer match. If the updated data on the target is not needed, perform a full or difference with block checksum mirror from the source to the target. If the updated data on the target is needed, restore the data from the target to the source.

Configuring failure monitoring

You will be establishing high availability by configuring Storage Mirroring failure monitoring. In the event of a failure, the target can stand in for the source with minimal disruption to end users.

1. If a failure occurs, you will want to have the Exchange services start on the target machine automatically. To do this, create a batch file on the target called `postover.bat` using the sample batch file below. Save the batch file to the same directory where your Storage Mirroring files are installed.

PostOver.BAT

```
rem   Sample Exchange 2000/2003 post-failover script.
rem   The following line pauses Storage Mirroring processing until the Storage Mirroring queue on the
target
rem   has been flushed. The time specified, in seconds, is a wait time that starts when the target
rem   queue becomes idle. If the wait time elapses, with no further activity in the queue, processing
rem   will continue. You will need to subsititute your target for target_name in the command.
"c:\program files\OpenView\Storage Mirroring\dtcl.exe" waitontarget target_name 10

rem   The following line sets a flag so that the database can be overwritten. You will need to
rem   replace source_name with the name of your source and target_name with the name of your target.
"c:\program files\OpenView\Storage Mirroring\exchfailover.exe" -setup -failover -s source_name -t
target_name

rem   The following lines start the Exchange services on the target. You may need to modify the
rem   script to fit the Exchange version and specific services used in your environment. If the service
rem   is running on the source, then you'll need to start it in this batch file. If the service is not
rem   running on the source, because it is disabled (like POP3Svc and IMAP4Svc are disabled by default
rem   in Exchange 2003), then you do not want to start the service in the batch file. If you modify the
rem   batch file to fit your environment, the services must still be started in the order shown. Just
rem   remark out the services that are not applicable to your environment. Because the Exchange
rem   services may return that they have started when in fact they have not, the DTCL wait command
rem   pauses processing to allow Exchange to complete its startup ensuring dependent services
rem   will not fail. The amount of time to set the wait command will vary from server to server.
rem   This sample script includes a 20 second interval but it may need to be adjusted to fit
rem   your environment. See the Storage Mirroring User's Guide for details on the wait command and
running
rem   DTCL from a command line. If desired, you can substitute the Microsoft sleep utility for the
rem   DTCL wait command. The sleep utility can be found in the Windows 200x resource kit.
net start MSExchangeSA
"c:\program files\OpenView\Storage Mirroring\dtcl.exe" wait 20000
net start MSExchangeIS
"c:\program files\OpenView\Storage Mirroring\dtcl.exe" wait 20000
net start MSExchangeMTA
"c:\program files\OpenView\Storage Mirroring\dtcl.exe" wait 20000
net start POP3Svc
net start IMAP4Svc
net start MSExchangeMGMT
net start RESvc
net start MSExchangeES
net start W3SVC
net start SMTPSVC

rem   The following line points the mailboxes in active directory to the target server. You will need to
rem   replace source_name with the name of your source and target_name with the name of your target.
"c:\program files\OpenView\Storage Mirroring\exchfailover.exe" -failover -s source_name -t target_name
```

NOTE: In some cases the Information Store (IS) may not start on the first attempt. If this happens, simply restart the service and it should start properly. (You will have to restart the other services in the same order as listed in the script.)

The Exchange Failover utility as used in the sample script above is only valid for simple Exchange configurations in which the mail store names (specifically the filename of its database, excluding path information) are unique. If your environment uses the same store name for different groups or if you need to rename stores or groups on the target during failover, you will need to add additional options to the Exchange Failover utility used in the `postover.bat` script. See "Appendix 3: Configuring additional Exchange Failover utility options" on page 25 for more information.

A copy of this sample script (`postover.bat.sample`) is available in the Samples folder, located in the directory where Storage Mirroring is installed. After you modify the sample script, copy the script and save it with a new name to remove the `.sample` extension.

If you are upgrading from an earlier version of the Exchange Failover utility, the failover and failback scripts can be modified to remove the NSISPN commands. This functionality has been incorporated into the utility and is no longer necessary in the scripts. Leaving the commands in the scripts will not cause any harm or failure in execution.

2. If your source server is the routing master, you will need to modify the security settings so that the routing master role can be moved to the target. If your source server is not the routing master, skip this step and continue with step 3.

   You have two options available for modifying the security settings for the routing master role.

   - The first option grants the Exchange Failover utility the permission to perform the task for you. Edit the `postover.bat` file that you just created and add the `-u username:password` switch as outlined in the table "Exchange Failover Utility command syntax" on page 28. Specify the Exchange administrator account information.
   - The second option allows you to set the security setting manually, thus not requiring the `-u` switch in the failover and failback scripts. You will have to use ADSIEdit from the Windows Support Tools to make this change. See your Windows reference guide for more information.

     a. Open ADSIEdit and go to `CN=Routing Groups, CN=First Administrative Group, CN=Administrative Groups, CN=Exchange_Organization_Name, CN=Microsoft Exchange, CN=Services, CN=Configuration, DC=Domain_name, DC=com`.

     b. Right-click on the entry, then choose **Properties**.

     c. Select the Security tab, then click **Advanced**.

     d. Click **Add**. Click on **Object Types** and verify that **Computers** are selected. Click **OK**.

     e. Type in your `target_name` and click **CheckName**.

     f. Select **Full Control**, then click **OK**.

3. After a failure is resolved, you will be ready to bring your source back online. At this time, you will want to stop the Exchange services on the target automatically and move users and roles. To do this, create a batch file on the target called `preback.bat` using the sample batch file below. Save the batch file to the same directory where your Storage Mirroring files are installed.

PreBack.BAT

```
rem   Sample Exchange 2000/2003 pre-failback script.

rem   The following lines stop the Exchange services on the target. You may need to modify
rem   the script to fit the Exchange version and specific services used in your environment,
rem   although the services must be stopped in the order shown.
net stop MSExchangeSA /y
net stop MSExchangeMGMT
net stop POP3SVC
net stop IMAP4SVC
net stop ResVC
net stop MSExchangeES
net stop W3SVC
net stop SMTPSVC

"c:\program files\OpenView\Storage Mirroring\exchfailover.exe" -failback -nopublicfolders -s source_name
-t target_name
```

NOTE: A copy of this sample script (`preback.bat.sample`) is available in the Samples folder, located in the directory where Storage Mirroring is installed. After you modify the sample script, copy the script and save it with a new name to remove the `.sample` extension.

If you are upgrading from an earlier version of the Exchange Failover utility, you will need to do the following:

- Compare the sample scripts to your failback and post-restore scripts and incorporate the new commands (`-nopublicfolders`, `-onlypublicfolders`) into your scripts.

Modify the failover and failback scripts to remove the NSISPN commands. This functionality has been incorporated into the utility and is no longer necessary in the scripts. Leaving the commands in the scripts will not cause any harm or failure in execution.

4. On the target, open the Failover Control Center. (**Start**, **Programs**, **Storage Mirroring**, **Failover Control Center**).
5. Select the target machine from the list of available machines. If the target you need is not displayed, click **Add Target**, enter the machine name, and click **OK**.
6. Click **Login** to login to the target machine.
7. To add a monitor for the selected target, click **Add Monitor**. Type the name of the source machine and click **OK**. The Monitor Settings window will open.
8. Select the IP address to be monitored by marking the check box to the left of the address in the **Names to Monitor** tree.
9. Select **IP Address(es)** and **Server Name** under **Items to Failover**.
10. If you are failing over/back the Active Directory hostname, click **Account** and specify a username and password with full domain administrative privileges.
11. Click **OK** to go back to the Monitor Settings dialog box.
12. Click **Scripts** and specify the location and file names of the scripts created earlier.
13. Click **OK** to go back to the Monitor Settings dialog box.
14. Click **OK** to begin monitoring the source machine.

In the event of a source machine failure, your target machine is now ready to stand in for the source.

NOTE: If you start Exchange Server and mount the replicated databases on the target, or if the data on the target is otherwise modified, the data on the source and target will no longer match. If the updated data on the target is not needed, perform a full or difference with block checksum mirror from the source to the target. If the updated data on the target is needed, restore the data from the target to the source.

Updating Exchange components after the initial configuration

After you have completed the initial configuration and Storage Mirroring is mirroring, replicating, and monitoring for a failure, your Exchange components on the source may not be static. You may need to add a new information store to your Exchange configuration, or you may need to update to a new Exchange service pack. In these cases, you do not need to repeat the entire initial configuration. Use the appropriate instructions below, depending on the change you need to make.

Adding a new information store

1. Pause transmission from the source to the target so that you can start Exchange on the target. From the Storage Mirroring Management Console on the source, right-click the established connection and select **Transmit**, **Pause**.
2. Start the Exchange services relevant to your environment on the target.
3. Create the information store on the target with the same name and location that will be created on the source.
4. Stop all of the Exchange services on the target that you started.
5. Back on the source, resume transmission by right-clicking the paused connection and selecting **Transmit**, **Resume**.
6. Create the information store on the source with the same name and location that were created on the target.

NOTE: If you selected a path that is outside of the existing replication set, you will need to modify the replication sets on the source and target to include the path(s) to the new data.

7. Again using the Storage Mirroring Management Console on the source, check the orphan settings for the established connection. Right-click the connection and select **Connection Manager**.
8. Select the Orphans tab and verify that you are either moving or deleting orphan files. For more information on orphan files, see the *HP OpenView Storage Mirroring user's guide*. Click **OK** to close the Connection Manager.
9. Perform a file differences block checksum mirror by right-clicking on the connection and selecting **Mirroring**, **Start**.
10. Select **File differences** and **Use block checksum** and click **OK**.

When the difference mirror is complete, the target will be ready to stand in for the source with the new information store.

Applying an Exchange service pack or upgrade

1. Stop the Storage Mirroring service on the source. Any data that was already transmitted from the source but is still in queue on the target will continue to process.
2. Apply the Exchange service pack or upgrade.
3. Verify that all of the data in queue on the target has been applied to the target before continuing. You can verify that the target queue is empty by checking the Bytes in Target Disk Queue statistic in the Target section of DTStat or the Bytes in Queue statistic in the Storage Mirroring Target section of Performance Monitor. If these statistics are zero (0), the queue is empty and you can continue. If these statistic are not zero, there is still data in queue on the target and you must wait before continuing. (For information on DTStat and Performance Monitor statistics, see the *HP OpenView Storage Mirroring user's guide*.)
4. Start the Exchange services relevant to your environment on the target.
5. Apply the same Exchange service pack or upgrade, making sure that any settings applied are identical to the source.
6. Stop all of the Exchange services on the target that you started.
7. Restart the Storage Mirroring service on the source. Storage Mirroring will automatically start a difference mirror to bring the data on the target up-to-date with data that may have changed on the source while you were going through this process.

When the difference mirror is complete, the target will be ready to stand in for the source with the updated components.

Dealing with a failure

If a failure occurs and the Failover Control Center Time to Fail counter reaches zero (0), a dialog box will appear in the Failover Control Center requiring user intervention to initiate failover. (If the Failover Control Center is not open when the failure occurs, the dialog box will appear the next time the Failover Control Center is opened and you are logged on to the target. See the *HP OpenView Storage Mirroring user's guide* for information on monitoring a failure.) Acknowledge the manual intervention prompt to start failover.

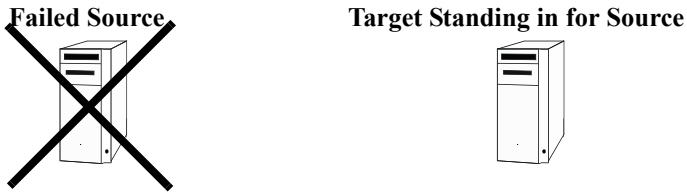
The failover script created earlier will automatically run. During failover, Windows Event Viewer, Storage Mirroring log, and Exchange Failover utility logs (located in the same directory as the Exchange Failover utility) record the failover events. When failover is complete, the target will have the Exchange services started, the databases mounted, and the users pointed to the target. At this time, clients can connect through Outlook or Outlook Web Access to receive their e-mail. Users that had Outlook open during the failure will need to restart the Outlook client (excluding Outlook Web Access clients on a LAN).

During a failover, you cannot create a new global address list because the forest-level Recipient Update Service is still pointing to the source server. Use the instructions below if you need to create a new global address list. If you do not need to create a new global address list while the target is standing in, you can disregard these instructions.

1. Using System Manager on the target, expand the Organization object, then expand the Recipients container.
2. Click **Recipient Update Service**.
3. In the left pane, right-click **Recipient Update Service (Enterprise Configuration)** and select **Properties**.
4. Next to the **Exchange Server** field, select **Browse**.
5. Locate the target server and click **OK**.
6. To manually initiate an update of the recipients in that domain, right-click the **Recipient Update Service** and click **Update Now** or **Rebuild** to force an update.

Recovering after a failure

If your source experiences a failure, such as a power, network, or disk failure, your target machine will stand in for the source while you resolve the source machine issues. During the source machine downtime, data is updated on the target machine. When your source machine is ready to come back online, the data is no longer current and must be updated with the new data on the target machine.

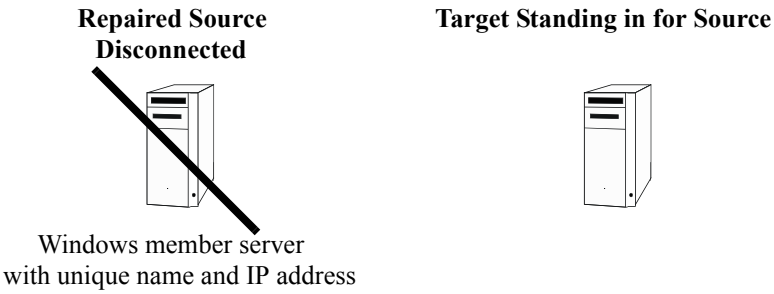


Before you begin to restore to the original source, resolve the issue(s) that caused the failure.

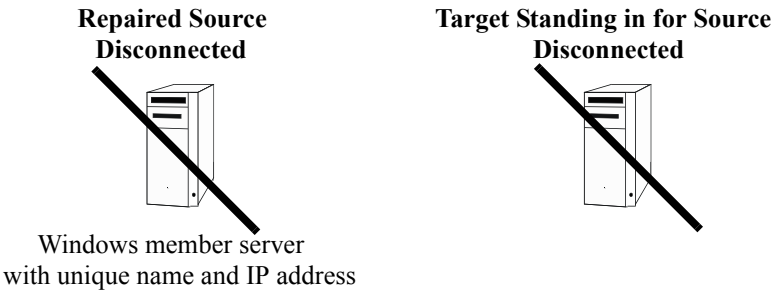
The recovery steps are different depending on the type of failure that occurred. If the source server has to be rebuilt, follow the instructions in "Rebuilding the source" on page 14. If the server is just offline due to non-disk related issues (such as network problems issues or power failure) and you do not need to rebuild your server, follow the instructions in "Recovering to the original source" on page 17.

Rebuilding the source

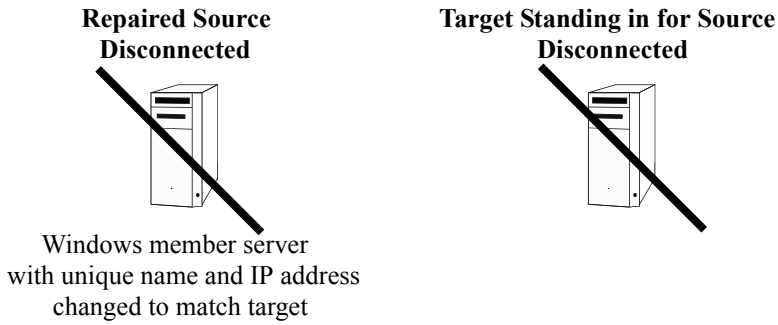
1. Install Windows on the source, if necessary, configuring it as a Windows 200x member server with a unique name and IP address. If you need to rebuild your source using the same server name, see "Appendix 2: Alternate recovery method" on page 24.



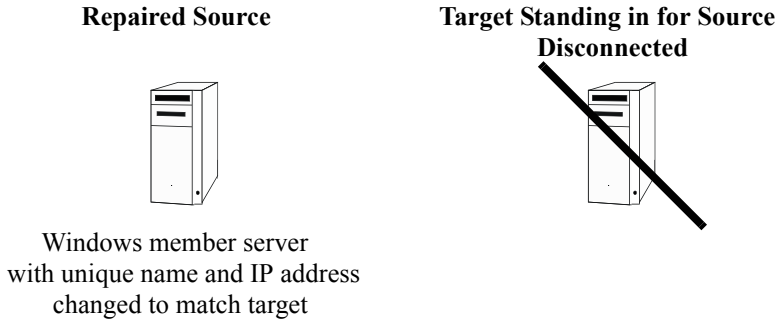
2. Apply any Windows 200x service packs or patches.
3. Temporarily, disconnect the target server from the network. At this time, users will no longer be able to access Exchange.



4. Change the source IP address to the target's assumed IP address. This is the source's original IP address before it failed.



5. Verify that the target is disconnected from the network, then connect the source to the network.



NOTE: You can automate steps 6-13 and avoid rebooting by running the following two commands in a script file. Netdom is included in the Windows 200x Support Tools, found in the Support directory on the Windows 200x CD. This utility allows you to add a machine into a domain. Modify the commands to fit the names used in your environment.

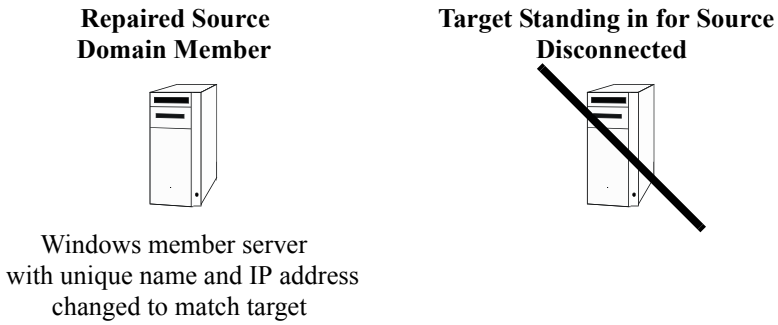
```
netdom join source_server_name /Domain:domain_name /UserD:user_name
/PasswordD:password
```

```
runas /user:user_name "cd_drive:\setup\i386\setup.exe /DisasterRecovery"
```

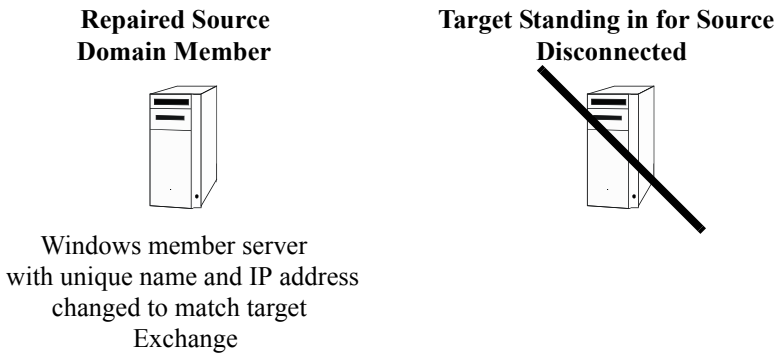
If you choose to automate steps 6-13, continue with step 14.

6. On the source, right-click **My Computer** and select **Properties**.
7. Select the Network Identification tab and click **Properties**.
8. Under **Member of**, change to **Domain** and specify the domain name.
9. Click **OK**.
10. When you are prompted for a domain account, specify an account with permissions to add a workstation to the domain.

11. Reboot when prompted.



12. After the source reboots, log in as the domain administrator or an equivalent account. Verify that the account has full Exchange Administrator rights.
13. Using the Exchange CD, start the Exchange installation on the source using the following command
`<cd drive>:\setup\i386\setup.exe /DisasterRecovery`
14. At the Component Selection dialog box, set the **Action** column to **Disaster Recovery** for all of the components that were originally installed on the source (before it failed).
15. Verify that each of the components selected are installed in the same location on the source as they are on the target and the original source. If not, modify the location of each component to match the target and original source configuration.
16. After selecting the proper components and location, click **Next** to continue the install.
17. If you accepted the default installation on the original source (before it failed), set Microsoft Exchange Messaging and Collaboration Services and Microsoft Exchange System Management Tools to **Disaster Recovery**.

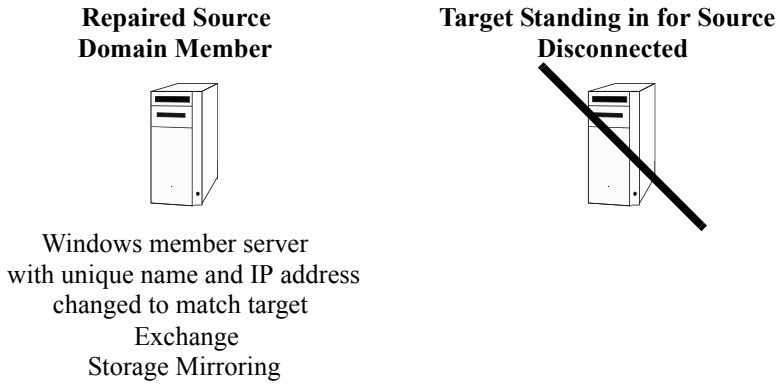


NOTE: Because the Exchange disaster recovery installation is configured for tape backup recovery, informational messages such as the following may appear; however, they do not apply to this configuration and can be disregarded:

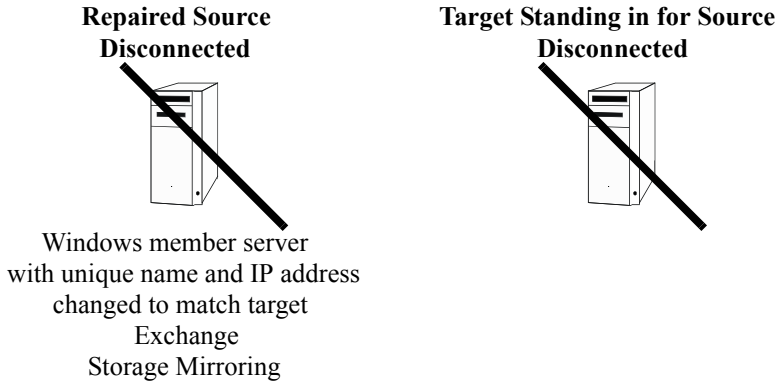
- `Use Exchange Admin Snap-in to ensure that you have a valid Exchange Server Object for this server for which you are running setup in recovery mode.`
- `After setup has completed, restore your databases from backup, then reboot your machine.`

During the post-installation processing, the installation may stall while trying to start the System Attendant (MSExchangeSA) service. It should take no more than a couple of minutes to start this service. If it takes longer, use the Windows Task Manager to terminate the setup process. This will not affect your ability to start services on the target after a failure.

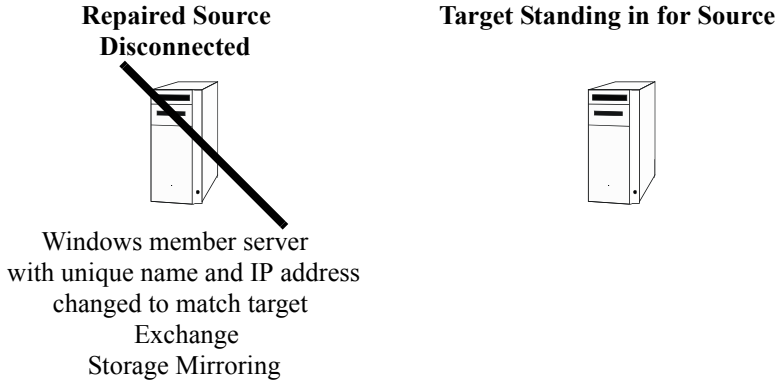
18. Install any Exchange service packs or patches.
19. Install Storage Mirroring, if necessary.



20. Remove the rebuilt source from the network.



21. Reconnect the target to the network.



22. Continue to the next section, "Recovering to the original source", to restore the data from the target back to the source.

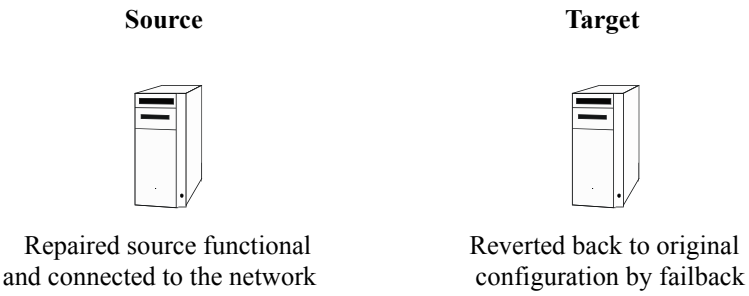
Recovering to the original source

1. Stop all of the Exchange services on the source so that you can overwrite the data with the newer data on the target. The services must be stopped in the order identified in the pre-failback script. See "PreBack.BAT" on page 11.

NOTE: If the services do not stop, you can manually terminate the processes through the Task Manager.

2. On the target, open the Failover Control Center (**Start**, **Programs**, **Storage Mirroring**, **Failover Control Center**).

3. Select the target machine that is currently standing in for the failed source.
4. Highlight the failed source and click **Failback**. The failback script created earlier will automatically run. During failback, Windows Event Viewer and the Storage Mirroring log record the failback events. When failback is complete, the Exchange services will be stopped on the target and the Failback Complete dialog box will appear.
5. **Do not** select **Continue** or **Stop** at this time. First, reconnect the source to the network.



6. After the source is available on the network, select **Continue** (to restart monitoring) or **Stop**.
7. To begin the restoration process, open the Storage Mirroring Management Console on the target (**Start**, **Programs**, **Storage Mirroring**, **Management Console**).
8. Login to the source machine by double-clicking on it.
9. Right-click on the original connection and select **Disconnect**.
10. Select **Tools**, **Restoration Manager**.
11. Complete the appropriate fields on the Restoration Manager.
    - **Original Source**—The source where the data originally resided.
    - **Restore From**—The target that contains the replicated data that users have been updating.
    - **Replication Set**—The name of the replication set
    - **Restore To**—The source where the data will be restored to.
12. Disable **Only if backup copy is more recent**. This option must be disabled because if the Exchange services were stopped on the source after the time they were stopped on the target, the source files will have a more recent date and time and the target files will not be restored.
13. Identify the correct drive mappings for the data and any other restoration options necessary. For detailed information on the restoration options, see the *HP OpenView Storage Mirroring user's guide*.
14. **On the Orphans tab, select to move or delete orphan files on the source.** Orphan files, such as out-dated transaction logs, may keep the database from starting on the source. For more information about orphan files, see the *HP OpenView Storage Mirroring user's guide*.
15. Verify that the selections you have made are correct and click **Restore**. The restoration procedure time will vary depending on the amount of data that you have to restore.

NOTE: When the restoration process is complete, the restoration status information will no longer appear in the right pane.

---

16. Continue to the next section, "Running the Exchange Failover utility", to complete the restoration process.

Running the Exchange Failover utility

After the restoration is complete, you will need to run the Exchange Failover utility to verify replica settings.

1. In a command prompt window on the source, change to the Storage Mirroring directory, then execute the following command:

   `exchfailover -setup -failback -s source_name -t target_name`

   where *source_name* is the name of the source and *target_name* is the name of the target.

2. Start the Exchange services on the source.
3. If you moved the routing master role to the target, you will need to modify the security settings so that the routing master role will be updated back to the source. You have two options available for modifying the security settings for the routing master role.
   - The first option grants the Exchange Failover utility the permission to perform the task for you. If you want to use this option, add the `-u username:password` switch as outlined in the table <cross reference>Exchange Failover Utility command syntax on page 28 to the `exchfailover` command in the following step. Specify the Exchange administrator account information.
   - The second option allows you to set the security setting manually, thus not requiring the `-u` switch in the failover and failback scripts. You will have to use ADSIEdit from the Windows Support Tools to make this change. See your Windows reference guide for more information.

     a. Open ADSIEdit and go to `CN=Routing Groups, CN=First Administrative Group, CN=Administrative Groups, CN=Exchange_Organization_Name, CN=Microsoft Exchange, CN=Services, CN=Configuration, DC=Domain_name, DC=com`.

     b. Right-click on the entry, then choose **Properties**.

     c. Select the Security tab, then click **Advanced**.

     d. Click **Add**. Click on **Object Types** and verify that **Computers** are selected. Click **OK**.

     e. Type in your `target_name` and click **CheckName**.

     f. Select **Full Control**, then click **OK**.
4. In a command window, execute the following command:

   `exchfailover -failback -onlypublicfolders -s source_name -t target_name`
   where *source_name* is the name of the source and *target_name* is the name of the target.

NOTE: Depending on your configuration, this command may take several minutes to run. The interface does not provide any visual notification that the failback is in process.

You can automate steps 1–5 by using the batch file "Sample Batch File to Automate Steps After Restore".

5. Restart any Outlook clients so that they can access the source.

   To reestablish protection of the Exchange data on the source, create a replication set, reestablish the Storage Mirroring connection to the target, and begin failure monitoring as documented earlier in the procedure.

Sample Batch File to Automate Steps After Restore

```
rem   Sample batch file to automate steps after restore.

rem   The user executing this batch file must have System permissions.

rem   The following line sets a flag so that the database can be overwritten. This step is actually
rem   repetitive of previous manual steps, because testing has found the database overwrite flag to
rem   often be inconsistent. You will need to replace source_name with the name of your source and
rem   target_name with the name of your target.
"c:\program files\OpenView\Storage Mirroring\exchfailover.exe" -setup -failback -s source_name -t
target_name

rem   The following lines start the Exchange services on the source. You may need to modify the
rem   script to fit the Exchange version and specific services used in your environment. If the service
rem   is running on the source, then you'll need to start it in this batch file. If the service is not
rem   running on the source, because it is disabled (like POP3Svc and IMAP4Svc are disabled by default
rem   in Exchange 2003), then you do not want to start the service in the batch file. If you modify the
rem   batch file to fit your environment, the services must still be started in the order shown. Just
rem   remark out the services that are not applicable to your environment. Because the Exchange
rem   services may return that they have started when in fact they have not, the DTCL wait command
rem   pauses processing to allow Exchange to complete its startup ensuring dependent services
rem   will not fail. The amount of time to set the wait command will vary from server to server.
rem   This sample script includes a 20 second interval but it may need to be adjusted to fit
rem   your environment. See the Storage Mirroring User's Guide for details on the wait command and
running
rem   DTCL from a command line. If desired, you can substitute the Microsoft sleep utility for the
rem   DTCL wait command. The sleep utility can be found in the Windows 200x resource kit.
net start MSExchangeSA
"c:\program files\OpenView\Storage Mirroring\dtcl.exe" wait 20000
net start MSExchangeIS
"c:\program files\OpenView\Storage Mirroring\dtcl.exe" wait 20000
net start MSExchangeMTA
"c:\program files\OpenView\Storage Mirroring\dtcl.exe" wait 20000
net start POP3Svc
net start IMAP4Svc
net start MSExchangeMGMT
net start RESvc
net start MSExchangeES
"c:\program files\OpenView\Storage Mirroring\dtcl.exe" wait 20000

rem   The following line points the mailboxes in active directory to the source server. You will need to
rem   replace source_name with the name of your source and target_name with the name of your target.
"c:\program files\OpenView\Storage Mirroring\exchfailover.exe" -failback -onlypublicfolders -s source_name
-t target_name
```

NOTE: A copy of this sample script (`post_restore.bat.sample`) is available in the Samples folder, located in the directory where Storage Mirroring is installed. After you modify the sample script, copy the script and save it with a new name to remove the `.sample` extension.

If you are upgrading from an earlier version of the Exchange Failover utility, you will need to do the following:

- Compare the sample scripts to your failback and post-restore scripts and incorporate the new commands (`-nopublicfolders`, `-onlypublicfolders`) into your scripts.

Modify the failover and failback scripts to remove the NSISPN commands. This functionality has been incorporated into the utility and is no longer necessary in the scripts. Leaving the commands in the scripts will not cause any harm or failure in execution.

Appendix 1: WAN configuration

Because failover of Exchange across a WAN is dependent on DNS and Active Directory, Exchange availability after failover is dependent on Active Directory and DNS updates. Therefore, additional configuration requirements and specific WAN configuration steps must be completed before the Exchange server will be available to users.

WAN requirements

The following additional requirements must be addressed if your source and target servers are on different subnets.

- Microsoft Exchange Server requires access to an Active Directory Domain Controller that is, at a minimum, configured as a Global Catalog Server.
- DNS Forward and Reverse lookup zones need to be properly configured per Microsoft standards.

Protecting your WAN Exchange data

You will need to complete the same four sections as the LAN configuration in order to protect your Exchange data. WAN-specific steps must be completed when configuring failure monitoring.

- Preparing the WAN source server—There are no unique steps when preparing a WAN source server. Complete the same steps as outlined in "Preparing the source server" on page 5.
- Preparing the WAN target server—There are no unique steps when preparing a WAN target server. Complete the same steps as outlined in "Preparing the target server" on page 6.
- Configuring Storage Mirroring mirroring and replication—There are no unique steps when configuring Storage Mirroring mirroring or replication on the WAN source server. Complete the same steps as outlined in "Configuring Storage Mirroring mirroring and replication" on page 8.
- Configuring failure monitoring—Follow the steps as outlined in "Configuring failure monitoring" on page 9, noting three changes that need to be made when configuring failure monitoring in a WAN environment:

1. On the Monitor Settings window, only select **Server Name** under **Items to Failover**. Do not select **IP Address(es)** to failover. This corresponds to step 9 in "Configuring failure monitoring" on page 9.

2. After failover and failback, you will need to update DNS. This can be done manually after the failover/failback is complete, or can be done during the failover process as part of the failover script postover.bat (step 1 in "Configuring failure monitoring" on page 9) and failback script `preback.bat` (step 3 in "Configuring failure monitoring" on page 9). Three possible options for updating DNS are outlined below.

   a. **Manual DNS updates**—You can update the DNS server manually by using the Windows Administrative Tools (Start, Programs, Administrative Tools, DNS).

   b. **Automated/Scripted updates using DNSCMD**—The DNS Server Troubleshooting Tool utility (DNSCMD), which can be found in the Windows 200x support tools, can be used in the Storage Mirroring failover and failback scripts to delete and add host and reverse lookup entries so that the source host name will resolve to the target IP address. The types of DNS records that will need to be modified vary by implementation but may include A, MX, and CNAME records.

      For example, the following commands would be added to the end of the failover script (`postover.bat`). The second and fourth lines are identical to what appears on the PTR record's properties in the Windows 200x DNS utility.

      ```
      dnscmd dns_server_name /RecordDelete domain_name source_name A
      source_IP_address /f
      dnscmd dns_server_name /RecordDelete reverse_subnet_IP.in-addr.arpa
      reverse_lookup_IP PTR source_server_name /f
      dnscmd dns_server_name /RecordAdd domain_name source_server_name A
      target_IP_address
      dnscmd dns_server_name /RecordAdd reverse_subnet_IP.in-addr.arpa
      reverse_lookup_IP PTR source_server_name
      dnscmd dns_server_name /RecordDelete domain_name @ MX 10
      Source_Name.domain_name /f
      dnscmd dns_server_name /RecordAdd domain_name @ MX 10
      Target_Name.domain_name
      ```

      For example, the following commands would be added to the end of the failback script (`preback.bat`). The second and fourth lines are identical to what appears on the PTR record's properties in the Windows 200x DNS utility.

      ```
      dnscmd dns_server_name /RecordDelete domain_name source_name A
      target_IP_address /f
      dnscmd dns_server_name /RecordDelete reverse_subnet_IP.in-addr.arpa
      reverse_lookup_IP PTR source_server_name /f
      dnscmd dns_server_name /RecordAdd domain_name source_server_name A
      source_IP_address
      dnscmd dns_server_name /RecordAdd reverse_subnet_IP.in-addr.arpa
      reverse_lookup_IP PTR source_server_name
      dnscmd dns_server_name /RecordDelete domain_name @ MX 10
      target_name.domain_name /f
      dnscmd dns_server_name /RecordAdd domain_name @ MX 10
      source_name.domain_name
      ```

      DNSCMD commands will only work if dynamic updates are enabled on the DNS zone. This is configured on the DNS zone Properties dialog box in the Windows Microsoft Management Console DNS snap-in. If **Only Secure Updates** is enabled (this option is available only on Active Directory integrated zones), the DNSCMD utility must be used in the context of a user who is in the domain DnsAdmins group. This means the Storage Mirroring service logon account must be in the DnsAdmins group if the commands are in failover and failback scripts. The Account option in the Storage Mirroring Monitor Settings does not apply to the failover and failback scripts, so verify the Storage Mirroring service logon account is in the DnsAdmins group.

The Windows Dynamic DNS (DDNS) client does not initiate a registration reflecting the failed over name and IP address when failover occurs, and the `ipconfig /registerdns` command will not cause the failed over name and IP address to be registered. Accordingly, host records for the source will remain intact after failover and any required changes must be made on all DNS servers used by relevant clients. Changes to non-Windows DNS servers and Windows DNS servers with dynamic updates disabled must be implemented by some other means, but since DNS zone files are text-based, they can be manipulated with any scripting language that can open, parse, and write to a text file.

c. **Automated/Scripted updates using DNS WMI**—The DNS WMI Provider can be used to automate or script adding and deleting records to and from the DNS server. The steps vary based on the operating system.

Windows 2000—For information on the DNS WMI Provider, visit `msdn.microsoft.com` and search for DNS WMI Provider. The following link can also be used:

msdn.microsoft.com/library/en-us/dns/dns/installing_the_provider.asp

To download the DNS WMI Provider, use the following link:

ftp.microsoft.com/reskit/win2000/dnsprov.zip

Once the DNS WMI Provider for Windows 2000 has been installed on the DNS Server, the included VBS scripts can be used to automate DNS record modifications.

Windows 2003—The DNS WMI Provider is installed and configured by default on Windows 2003 DNS Servers, but the scripts necessary to modify DNS records are not pre-installed. Windows Server 2003 users will still need to download DNS WMI Provider for Windows 2000, which can be found at the following link:

ftp.microsoft.com/reskit/win2000/dnsprov.zip

Dealing with a WAN failure

Just like the LAN environment, if a failure occurs and the Failover Control Center Time to Fail counter reaches zero (0), a dialog box will appear in the Failover Control Center requiring user intervention to initiate failover. Since your source and target servers are in a WAN environment, update your DNS records on the target so that the source points to the target's IP address. Then, acknowledge the manual intervention prompt to start failover.

Again, like the LAN environment, the failover script created will automatically run. The target will have the Exchange services started, the database mounted, and the user pointed to the target. If you did not script DNS updates in the failover script, perform the manual DNS updates at this time. When those updates are completed, clients can connect through Outlook or Outlook Web Access to receive their e-mail.

Recovering after a WAN failure

Follow the steps as outlined in "Rebuilding the source" on page 14, noting that there is one additional step. After step 1 and the source machine problems that caused the failure have been resolved, update the DNS records so that the source name resolves to the original source IP address. All of the remaining steps are the same for a WAN environment. When failback occurs, clients who were accessing Exchange on the target at the time of failback may have to wait until their DNS cache is flushed and repointed to the source, or they can force the flush by using the `ipconfig /flushdns` command.

Appendix 2: Alternate recovery method

If you do not want to use a unique name when rebuilding the original source, use the following instructions.

1. On the target, open the Failover Control Center (**Start**, **Programs**, **Storage Mirroring**, **Failover Control Center**).
2. Select the target machine that is currently standing in for the failed source.
3. Highlight the failed source and click **Failback**. The failback script created earlier will automatically run. During failback, Windows Event Viewer and the Storage Mirroring log record the failback events. When failback is complete, the target will have the Exchange services stopped and the users repointed back to the source that you will be rebuilding.
4. Reconnect the source to the network.
5. On the target, when prompted to stop or continue monitoring of the source, select **Stop**.
6. Install Windows on the source, if necessary, configuring it as a Windows 200x member server with the same name and IP address as the original source.
7. Apply any Windows 200x service packs or patches.
8. Install Storage Mirroring, if necessary.
9. Connect the source to the network and join the domain.
   a. On the source, right-click **My Computer** and select **Properties**.
   b. Select the Network Identification tab and click **Properties**.
   c. Under **Member of**, change to **Domain** and specify the domain name.
   d. Click **OK**.
   e. When you are prompted for a domain account, specify an account with permissions to add a workstation to the domain.
   f. Reboot when prompted.
10. After the source reboots, log in as the domain administrator or an equivalent account. Verify that the account has full Exchange Administrator rights.
11. Using the Exchange CD, start the Exchange installation on the source using the following command:

    ```
    <cd drive>:\setup\i386\setup.exe /DisasterRecovery.
    ```

12. At the Component Selection dialog box, set the **Action** column to **Disaster Recovery** for all of the components that were originally installed on the source (before it failed).
13. Verify that each of the components selected are installed in the same location on the source as they are on the target. If not, modify the location of each component to match the target and original source configuration.
14. After selecting the proper components and location, click **Next** to continue the install.

15. If you accepted the default installation on the original source (before it failed), set Microsoft Exchange Messaging and Collaboration Services and Microsoft Exchange System Management Tools to **Disaster Recovery**.

NOTE: Because the Exchange disaster recovery installation is configured for tape backup recovery, informational messages such as those below do not apply to this configuration and can be disregarded.

Use Exchange Admin Snap-in to ensure that you have a valid Exchange Server Object for this server for which you are running setup in recovery mode.

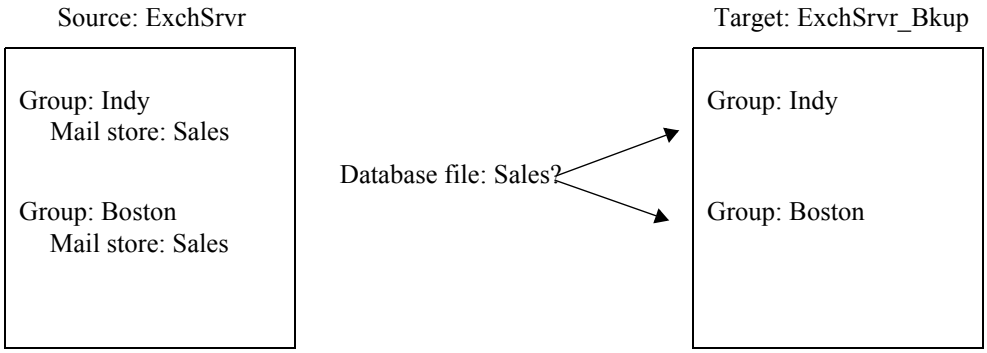
After setup has completed, restore your databases from backup, then reboot your machine.

16. During the post-installation processing, the installation may stall while trying to start the System Attendant (MSExchangeSA) service. It should take no more than a couple of minutes to start this service. If it takes longer, use the Windows Task Manager to terminate the setup process. This will not affect your ability to start services on the target after a failure.
17. Install any Exchange service packs or patches.
18. Stop all of the Exchange services on the source so that you can overwrite the data with the newer data on the target. The services must be stopped in the order identified in the pre-failback script. See "PreBack.BAT" on page 11.
19. To complete this process, continue with step 8 under "Recovering to the original source" on page 17 and complete the remaining steps in that section.

Appendix 3: Configuring additional Exchange Failover utility options

In order for a mail store (and its users) to be failed over (or failed back), a mail store on the source must be paired to a mail store on the target. In order to be a valid pair, the database filename (excluding path information) of these two stores must match. The Exchange Failover utility uses two methods to make these mail store pairs. The simplest (default) method requires that the database filenames be unique and that each filename only occurs once on the source and once on the target. This is the case for the example script provided in "Configuring failure monitoring" on page 9. If your environment uses the same store name in different groups or if you need to rename stores or groups on the target during failover, you will need to add additional options to the Exchange Failover utility used in the `postover.bat` script.

For example, a server called ExchSrvr contains two mail groups Indy and Boston. Each group contains a mail store called Sales. In its simplest form, the Exchange Failover utility would not know which group to associate the Sales mail store with since it is based on the database file name.



To resolve this issue, you can direct the groups and mail stores to meet your environment needs. The `-r` option in the Exchange Failover utility is a pairing rule. It allows you to specify how the groups and mail stores on the source will be paired on the target.

By itself, the `-r` option will create a one-to-one mapping from the source to the target. For example, the command

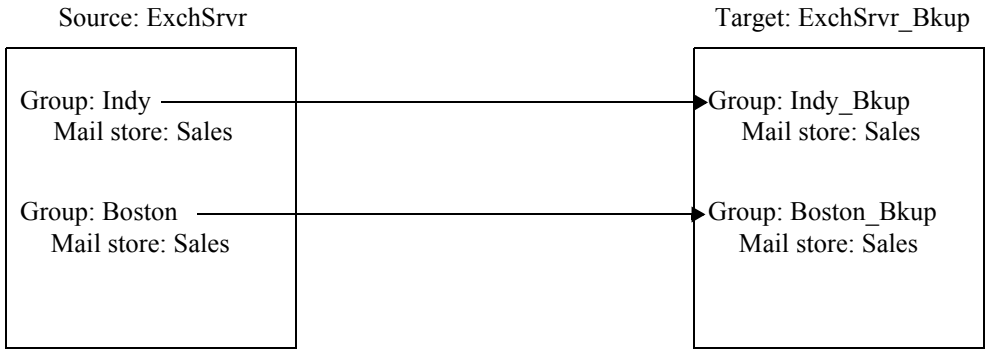
```
exchfailover.exe -failover -s ExchSrvr -t ExchSrvr_Bkup -r
```

would automatically create a one-to-one mapping on the target.

You can be more specific with the `-r` option and direct the source groups to specific group names on the target. For example, the command

```
exchfailover.exe -failover -s ExchSrvr -t ExchSrvr_Bkup -r Indy:Indy_Bkup -r
Boston:Boston_Bkup
```

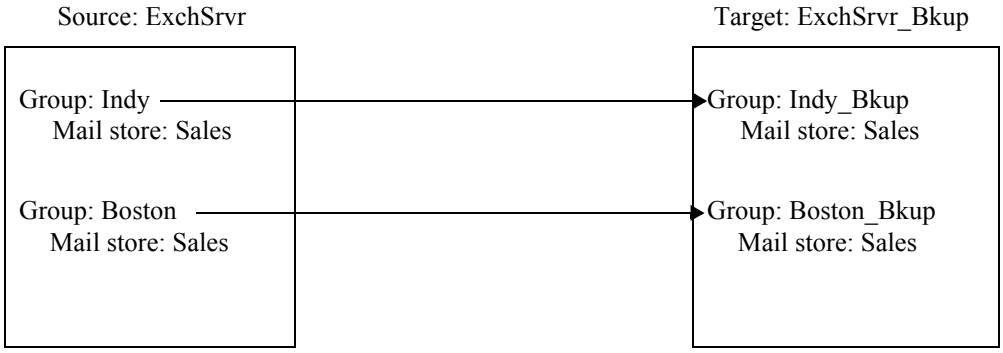
will pair the mail stores from the source Indy group in the group Indy_Bkup on the target. The mail stores from the source Boston group will be paired in the group Boston_Bkup on the target.



If needed, you can be the most specific with the `-r` option by specifying both the group and mail store names. For example, if you need to direct the group and mail store names on the target, the command

```
exchfailover.exe -failover -s ExchSrvr -t ExchSrvr_Bkup -r Indy,
Sales:Indy_Bkup, Sales -r Boston, Sales:Boston_Bkup, Sales
```

will pair the mail store Sales in the Indy_Bkup group from the Sales mail store from the Indy group on the source. It will also pair the mail store Sales in the Boston_Bkup group from the Sales mail store from the Boston group on the source.



There are several other options available in the Exchange Failover utility. These options and the full command syntax are included in "Exchange Failover Utility command syntax" on page 28.

Exchange Failover Utility command syntax

Command EXCHFAILOVER

Description Used in script files to failover Exchange data

Syntax

```
EXCHFAILOVER -FAILOVER | -FAILBACK -s <source> -t <target> [-l
<log_filename>] [-norus] [-nospn] [-nopublicfolders] [-onlypublicfolders]

[-o <options_filename>]
[-r [<source_group>][,<source_mail_store>][:[<target_group>]
[,<target_mail_store>]]] [-SETUP] [-test] [-u <username>:<password>] [-?[?]]
```

Options

- FAILOVER—The Exchange data will be moved from the source to the target during failover
- FAILBACK—The Exchange data will be moved from the target to the source during failback
- s *source*—The name of the original source server
- t *target*—The name of the original target server
- l *log_filename*—The name of the optional log file name. By default, the log file is ExchFailover.log and is stored in the directory containing the exchfailover.exe file. If this name is changed, the DTInfo utility will not be able to locate this file which could impede assistance through Technical Support.
- norus—Do not change the Recipient Update Service
- nospn—Do not change the Service Principle Name
- nopublicfolders—Do not move the public folders
- onlypublicfolders—Only move the public folders
- o *options_filename*—Allows you to pass in a file containing the options for the Exchange Failover utility
- r—By itself, this option creates a one-to-one mapping of the groups and mail stores from the source to the target
- r *source_group:target_group*—The r option with the group names will direct the source group name specified to the target group name specified
- r *source_group, source_mail_store:target_group, source_mail_store*—The r option with all of the r options will direct the source group name and mail store specified to the target group name and mail store specified
- SETUP—Allows you to set the overwrite database on restore flag without completing user moves or RUS and folder updates. If the -setup switch is not supplied, the utility still sets the overwrite database on restore flag, but the other work is performed also.
- test—Test mode that does not change the Exchange configuration
- u *username:password*—A user with Active Directory permissions
- ?—Displays the syntax of the Exchange Failover utility
- ??—Displays the syntax of the Exchange Failover utility along with brief descriptions of each option

Examples

- `exchfailover -failover -s Indy -t ExchSrvr_Bkup`
- `exchfailover -failover -s Indy -t ExchSrvr_Bkup -r`
- `exchfailover -failover -s Indy -t ExchSrvr_Bkup -r Sales:Indy_Sales`
- `exchfailover -failover -s Indy -t ExchSrvr_Bkup -r Sales, Inside:Indy_Sales, Inside -r Sales, Outside:Indy_Sales, Outside`
- `exchfailover -failover -s Indy -t ExchSrvr_Bkup -r Sales:Indy_Sales -norus -u administrator:password`
- `exchfailover -failover -s Indy -t ExchSrvr_Bkup -o options_file.txt`

Notes

- When using the `-failback` option, the source-related options pertain to your original source or what will become the new source, if the original source had to be replaced. The target-related options pertain to the target that is currently standing in for the source.
- The password specified with the `-u` option is the only case-sensitive option in this command.

Appendix 4: Security requirements

When performing failover operations, the Storage Mirroring software is designed to operate with Failover Control Center running under the `LocalSystem` account, which is the same as the Microsoft Exchange System Attendant service. This configuration should provide sufficient permissions for most operations that occur during failover, including DNS updates, SPN updates, changes to the Active Directory schema, and updating mailbox properties for each user.

NOTE: Depending on your environment, a lower level of permissions may be applied.

SPN updates

Failover

During failover, the source server's Active Directory SPNs will be moved to the target server's Active Directory object. In order to accomplish this, the `Write servicePrincipalName` permission on the source's computer account in Active Directory must be assigned to the account that will modify the SPNs, which can be either of the following:

- The target's Storage Mirroring service logon account. If the target's Storage Mirroring service is configured to log on as the System account, the target's Active Directory computer account should be assigned the permissions.
- The account specified in the failover monitor configuration

Write or Full Control permissions (which are assigned to Domain Administrators by default) can also be used to assign `Write servicePrincipalName` permissions.

Use the following procedure to assign the `Write servicePrincipalName` permission to a user or group.

1. Open ADSIEdit and go to `CN=Server_Name,CN=Computers,DC=Domain_name,DC=com`.
2. Right-click on the entry, then choose **Properties**.
3. Select the Security tab, then click **Advanced**.
4. Click **Add**. Click on **Object Types** and verify that **Computers** is selected. Click **OK**.
5. Type in your `target_name` and click **CheckName**.
6. Select **Full Control**, then click **OK**.

Failback

During failback, the `Write servicePrincipalName` permission on the target's computer account in Active Directory must be assigned back to the account that will modify the SPNs on the source.

To update the permissions on the source, follow the SPN Failover procedure, except assign Full Control to your `source_name` instead.

Routing master

Failover

If your source server is the routing master, you will need to modify the security settings so that the routing master role can be moved to the target. There are two options available for modifying the security settings for the routing master role:

- Use the `-u` parameter and specify an ID that has sufficient authority to perform the operations.
- Change specific Active Directory attributes to allow the update to be performed by the scripts run from the Failover Control Center.

You must use ADSIEdit (from the Windows Support Tools) to assign the correct permissions to allow for the updating of the Routing Master.

1. Open ADSIEdit and go to `CN=Routing Groups,CN=Computers,DC=Domain_name,DC=com`.
2. Right-click on the entry, then choose **Properties**.
3. Select the Security tab, then click **Advanced**.
4. Click **Add**. Click on **Object Types** and verify that **Computers** is selected. Click **OK**.
5. Type in your `target_name` and click **CheckName**.
6. Select **Full Control**, then click **OK**.

Failback

If your source server was the routing master, you will need to modify the security settings so that the routing master role can be returned.

To update the permissions on the source, follow the Routing Groups Failover procedure, except assign Full Control to your `source_name` instead.

Recipient Update Service

Failover

The target machine must have the ability to modify the Recipient Update Service information. This involves allowing specific permissions to the Exchange Organization.

1. Open ADSIEdit and go to `CN=Exchange_Organization_Name, CN=Microsoft Exchange, CN=Services, CN=Configuration, DC=Domain_name, DC=com`.
2. Right-click on the entry, then choose **Properties**.
3. Select the Security tab, then click **Advanced**.
4. Click **Add**. Click on **Object Types** and verify that **Computers** is selected. Click **OK**.
5. Type in your `target_name` and click **CheckName**.
6. Select **Full Control**, and click **OK**.

Failback

During failback, the ability to modify the Recipient Update Service information must be assigned back to the source.

To update the permissions on the source, follow the Recipient Update Service Failover procedure, except assign Full Control to your `source_name` instead.